Quantum-Resilient Key and Identity Lifecycle Architecture for Lightweight IIoT Systems

Chimeremma Sandra Amadi, Taesoo Jun
Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea
chimesandra@yahoo.com, taesoo.jun@kumoh.ac.kr

***Abstract*—Post-quantum cryptography (PQC) is fast becoming a necessity for the Industrial Internet of Things (IIoT), where security requirements must align with strict latency and resource constraints. Traditional security protocols relying on static identities, centralized revocation, and bulky ciphertexts are ill-suited for dynamic and distributed IIoT systems. This paper introduces a quantum-resilient identity and key management architecture optimized for constrained industrial environments. We propose a lightweight entropy-seeded identity model that leverages biometric, device, and environmental randomness to generate spoof-resistant identities. A compressed key encapsulation delivery protocol based on CRYSTALS Kyber512 is developed using delta encoding, fragmentation, and ZLIB compression to minimize ciphertext overhead. Although a hybrid blockchain integration is conceptually discussed to outline revocation and trust enforcement, our implementation on constrained IIoT devices demonstrates over 48% ciphertext size reduction, 30% latency improvement compared to baseline Kyber, and real-time trust scoring based on behavioral analysis, showing strong potential for scalable, bandwidth-aware, and future-proof security deployment in post-quantum IIoT ecosystems.**

***Index Terms*—Compressed Key Encapsulation, CRYSTALS-Kyber512, Entropy-Seeded Identity, Industrial Internet of Things (IIoT), Lightweight Security Framework, Post-Quantum Cryptography (PQC).**

I. Introduction

As the global shift toward post-quantum cryptography (PQC) accelerates, industrial systems must urgently adopt identity and key management models that withstand quantum-enabled threats without compromising performance or interoperability. Traditional cryptographic schemes are increasingly inadequate especially in the Industrial Internet of Things (IIoT), where secure identity, low-latency communication, and trust lifecycle management are critical. Despite projections of over 29 billion industrial devices by 2025, fewer than 15% are equipped with PQC protections [1], underscoring the need for lightweight, quantum-resilient security solutions. This work introduces a unified architecture that integrates two essential security layers, an entropy-seeded identity generation mechanism, leveraging biometric, behavioral, and environmental randomness to produce unique, hardware-rooted identities; and a delivery-aware PQC protocol that applies delta-based compression to Kyber512 ciphertexts, enabling secure yet bandwidth-efficient key exchange for constrained IIoT nodes. Entropy-seeded identities have emerged as a promising strategy to mitigate identity spoofing and static credential reuse.

Studies such as [2], [3], and [4] demonstrate the effectiveness of PUF-based and entropy-driven approaches in low-power environments. However, these methods often operate in isolation, lacking integration with PQC delivery mechanisms or blockchain-based lifecycle controls. Historically, IIoT security architectures have treated identity provisioning, encryption, and revocation as discrete stages using static credentials at provisioning, conventional TLS-based key exchange, and centralized or manual revocation workflows. While functionally sufficient in the past, these siloed systems now reveal fundamental weaknesses where static keys are prone to impersonation, revocation mechanisms are slow and non-transparent, and bulky PQC ciphertexts strain resource-limited devices. This fragmentation introduces latency, coordination overhead, and systemic vulnerabilities particularly in distributed and dynamic industrial environments. Fig 1, shows a non-unified IIoT security framework having quantum seeded identity, secure key delivery and blockchain revocation mechanism.

The proposed integration addresses these challenges holistically. By unifying entropy-rooted identity generation with delivery-optimized PQC encapsulation, and extending toward a scalable revocation model, we transition from reactive security to adaptive trust management. This lifecycle-aware design reduces redundancy, improves coordination, and aligns with the tight resource budgets of IIoT platforms. As highlighted by [5] and [6], ciphertext size and delivery efficiency remain practical obstacles to PQC adoption obstacles our compression scheme directly mitigates. At the revocation and auditability layer, we conceptually propose a hybrid blockchain framework that combines the control of private ledgers with the transparency of public chains. Smart contracts facilitate real-time identity transitions and trust scoring, while quantum-secure signatures protect the integrity of revocation and trust updates.

Prior efforts such as [7], [8], and [9] illustrate the benefits of blockchain-based lifecycle enforcement, yet our approach is unique in its proposed dual-chain architecture tailored for IIoT trust propagation. By tightly coupling identity and PQC layers rather than treating them as standalone modules our system enables predictive revocation, dynamic trust evolution, and scalable deployment. While the blockchain component is not fully implemented in this study, its conceptual integration is outlined to guide future research on end-to-end trust architectures in quantum-resilient IIoT systems. The key contributions of this work are as follows:

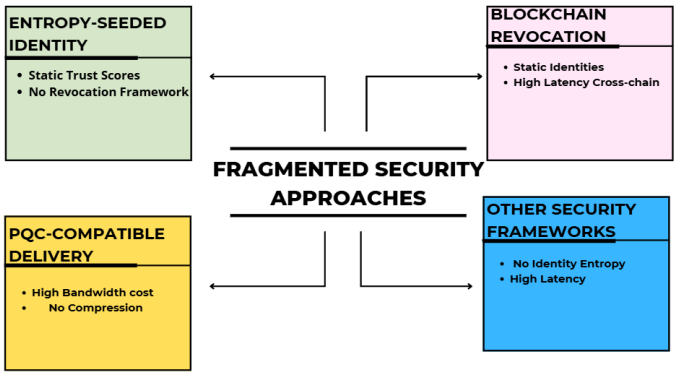

Fig. 1. Non-unified Systems of IIoT security frameworks having Quantum Seeded Identity, Secure Key Delivery and Blockchain Revocation

- We propose an entropy-seeded identity model that fuses biometric features, device-level metadata, and system-derived randomness to generate statistically unique identity digests. These digests serve as trust anchors for quantum-resilient authentication and enable real-time trust evolution.
- We design a lightweight, reuse-aware ciphertext compression protocol tailored for CRYSTALS-Kyber512, incorporating delta-based encoding and fragment-level redundancy elimination to reduce post-quantum delivery overhead without compromising security or decryptability.
- We validate the implementation on constrained IIoT hardware and demonstrate the feasibility of real-time key exchange and identity updates under quantum-safe cryptographic constraints. A simulated anomaly detection scenario illustrates the dynamic trust scoring capability of our identity model.
- We outline a hybrid blockchain-based revocation framework to illustrate the lifecycle integration of post-quantum trust enforcement. While this blockchain component is not fully implemented in the current version, its role in enabling decentralized identity tracking and revocation is articulated for future work.

The convergence of entropy driven identity models and compressed post-quantum delivery schemes offers a promising pathway for scalable and resilient IIoT security. While this work prioritizes the implementation and validation of these two core components, we also briefly outline a complementary blockchain-based revocation layer to demonstrate the architectural completeness of the proposed framework. The hybrid blockchain system comprising private and public chains for lifecycle enforcement remains conceptual within this paper scope, with full implementation reserved for our extended journal publication.

II. System Design and Methodology

This section outlines the overall system design, as illustrated in Fig. 2, all functional modules, including the entropy-seeded identity engine, compressed Kyber-based KEM delivery, and a cross-chain blockchain bridge for revocation enforcement. However, only the identity generation and delivery optimization modules are implemented and validated. The blockchain module is shown to illustrate lifecycle alignment but is left as a future implementation step, to be explored in detail in our journal extension. The proposed architecture is a multi-component framework engineered to enhance post-quantum security for IIoT environments. It integrates four core modules, entropy-seeded identity generation, compressed key encapsulation mechanism (KEM), fragmentation and reuse-aware delta compression, and hybrid blockchain-based revocation bridge. At the foundation lies the entropy-seeded identity generator, which collects biometric data, revocation history, device metadata, and real-time trust metrics. This diverse input forms a high-entropy pool used to generate unique, context-aware, and spoof-resistant identity digests that anchors subsequent cryptographic operations:

$$ID = \text{Hash}(\text{Fingerprint} \parallel \text{Revocation} \parallel \text{Metadata} \parallel \text{Trust}) \tag{1}$$

To minimize transmission overhead, we implement a reuse-aware compression scheme that avoids retransmitting known ciphertext segments. Let K be the original key and R_i denote reusable fragments. The compressed key K' is expressed as:

$$K' = \bigcup_{i=1}^{n} R_i + \Delta K \tag{2}$$

where ΔK contains only the delta new or changed bits enabling efficient key reconstruction on the receiver side. The KEM delivery module employs Kyber512 to establish post-quantum secure shared secrets. Ciphertexts are fragmented and compressed using ZLIB, reducing bandwidth while preserving decryption integrity. These compressed payloads are then transmitted to the receiving device or forwarded to the trust lifecycle manager. Finally, the system conceptually incorporates a cross-chain blockchain bridge to enforce revocation and trust updates.

A. Proposed Entropy-seeded Identity Model

In the context of Industrial IoT (IIoT) systems, device identity must be both unpredictable and tamper-resistant, especially under post-quantum threat models. To ensure such resilience, we propose an entropy-seeded identity model that derives the cryptographic identity from a combination of time-sensitive, device-specific, and entropy-rich input sources. The cryptographic identity $\text{ID}_{\text{device}}$ is generated by hashing a secure entropy pool, ensuring uniqueness across time and device instances. The formulation is given as:

$$\text{ID}_{\text{device}} = \text{SHA256}(H_{\text{entropy}} \parallel \text{timestamp} \parallel \text{device\_token}) \tag{3}$$

Where:

- H_{entropy} is a high-entropy value harvested from a system-level or hardware-based True Random Number Generator (TRNG), optionally seeded with biometric or behavioral randomness.

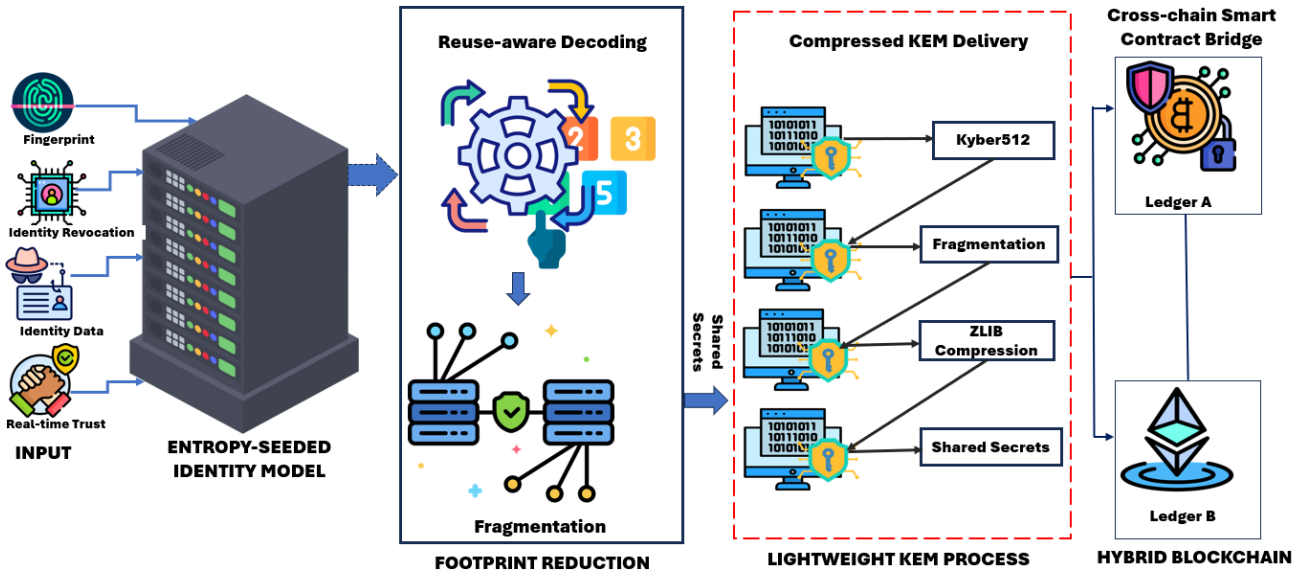

Fig. 2. Proposed Entropy-seeded Identity and Lightweight Model for resource-constrained industrial IoT environments highlighting the flow of input, process components.

- `timestamp` refers to the current Unix time at identity generation, introducing temporal uniqueness and preventing replay.
- `device_token` is a cryptographic fingerprint extracted from device-specific hardware properties such as MAC address, PUF responses, or fused identity values.

During device onboarding, this identity is anchored to the trust ledger or blockchain infrastructure, enabling persistent linkage with revocation, behavioral scoring, and trust evolution. In this formulation,there is a guarantee of forward security, as any compromise of past identities does not aid in predicting future identities due to non-deterministic entropy refresh. Then resistance against spoofing and cloning, since each device generates a non-reproducible identity digest even under identical environmental conditions.

TABLE I
MAPPING OF ENTROPY SOURCES TO SECURITY PROPERTIES

Entropy Source	Uniqueness	Freshness	Spoof Resistance
Biometric Fingerprint	✓	–	✓
Timestamp	–	✓	–
MAC Address	✓	–	–
TRNG (Hardware RNG)	✓	✓	✓
Revocation Logs	–	✓	✓
Trust Score Metrics	–	✓	–

Table I presents a structured mapping between the selected entropy sources used in the identity generation process and the specific security properties they reinforce. This mapping is critical to ensuring that the generated device identities are not only cryptographically strong but also context-aware and dynamically verifiable, For instance, biometric inputs introduce user-specific uniqueness, timestamps ensure temporal freshness, and TRNGs inject unpredictability essential for post-quantum resilience. By combining these sources, the system guarantees that no single entropy factor becomes a security bottleneck.

B. Compressed Key Encapsulation Delivery Protocol

To optimize post-quantum key exchange for resource-constrained IIoT devices, we propose a bandwidth efficient delivery scheme that applies delta compression and fragment-level reuse to Kyber512 ciphertexts. This protocol significantly reduces transmission overhead without compromising cryptographic security. The core mechanism performs delta encoding between the current ciphertext C and the previously transmitted ciphertext C_{prev}. The XOR operation captures the difference, and the resulting delta is compressed using the ZLIB compression library:

$$C' = \text{Compress}(C, C_{\text{prev}}) = \text{ZLIB}(C \oplus C_{\text{prev}}) \tag{4}$$

Where:

- C is the current Kyber512 ciphertext,
- C_{prev} is the ciphertext from the previous session,
- $\oplus$ denotes bitwise XOR for delta computation.

On the receiver end, reconstitution involves reversing the compression and XOR operations. Once the full ciphertext C is recovered, the shared secret `ss` is extracted via standard Kyber decapsulation using the private key sk:

$$C = C' \oplus C_{\text{prev}} \Rightarrow \texttt{ss} = \text{Decapsulate}(C, sk) \tag{5}$$

To further enhance efficiency, the ciphertext C is partitioned into n fixed-size fragments:

$$F = \{f_1, f_2, ..., f_n\} \tag{6}$$

Each fragment f_i has a uniform size k, allowing granular updates. During subsequent communication sessions, only the

modified fragments f_i' where changes occur are transmitted. The total transmission cost T is thus calculated as:

$$T = \sum_{i=1}^{n} \delta_i \cdot k \tag{7}$$

Here, δ_i is a binary indicator function defined as:

$$\delta_i = \begin{cases} 1, & \text{if } f_i \text{ changed} \\ 0, & \text{otherwise} \end{cases}$$

This model permits the receiver to reuse previously received fragments for unmodified sections, further conserving bandwidth. The overall compression efficiency is quantified using the compression ratio:

$$\text{Compression Ratio} = \frac{T}{n \cdot k} = \frac{\text{Modified Fragments}}{\text{Total Fragments}} \tag{8}$$

By leveraging fragment reuse and delta compression, the delivery-aware encapsulation strategy enables lightweight post-quantum communication, effectively reducing the payload size and making Kyber512 viable for ultra-constrained IIoT deployments.

C. Hybrid Blockchain Integration

The hybrid blockchain integration is discussed conceptually here to complete the architectural vision, but its practical implementation is deferred to future work. For secure revocation and alert propagation, a cross-chain bridge ensures synchronization between private and public ledgers. Revocation is triggered if a quantum-safe signature is verified:

$$\text{if } V_{\text{sig}}(A, M, \sigma) = \text{true} \Rightarrow \text{Revoke}(A) \in C_{\text{public}} \tag{9}$$

Where:

- V_{sig} is the quantum signature verification function,
- A is the identity address,
- M is the signed message,
- σ is the post-quantum signature,
- C_{public} is the Ethereum-based revocation contract.

This ensures trust synchronization and revocation auditability across ledgers.

D. Setup and Configuration

Table II provides the setup for the experimental prototype that was developed and tested in a hybrid environment consisting of Windows 11 with Ubuntu 24.04 LTS running through WSL2, using a machine equipped with an Intel Core i7 processor and 16GB of RAM. The cryptographic operations were powered by the PQClean library implementation of Kyber512, ensuring post-quantum security standards.

III. Results and Discussion

The following results pertain to the implemented components: entropy-seeded identity modeling, compressed post-quantum ciphertext delivery using Kyber512, and reuse-aware decoding. The hybrid blockchain bridge though essential to the proposed lifecycle is not implemented in this study and thus excluded from performance metrics. To validate the proposed system effectiveness on constrained IIoT endpoints, we carried out a series of microbenchmark tests using a Raspberry Pi 4 Model B with 4GB RAM, running Raspbian OS. The tests focus on dynamic trust score updates, key encapsulation performance, and compression efficiency.

TABLE II
Experimental Environment Configuration

Component	Specification / Tool Used
Operating System	Windows 11 with WSL2 (Ubuntu 24.04 LTS)
Hardware	Intel Core i7 Processor, 16GB RAM
Cryptography Library	PQClean implementation of `Kyber512`
Compression Library	`zlib` v1.2.13
Programming Language	C (compiled with GCC)
Blockchain Frameworks	• Hyperledger Fabric; private identity lifecycle management • Ethereum (Ganache Testnet); public telemetry and revocation audit
Visualization Tools	Python, Gnuplot

A. Entropy-seeded Identity Framework

To validate the proposed entropy-seeded identity framework, we implemented a prototype using Kyber512 to generate device keys, manage real-time trust evolution, and enforce predictive revocation based on behavioral anomalies.

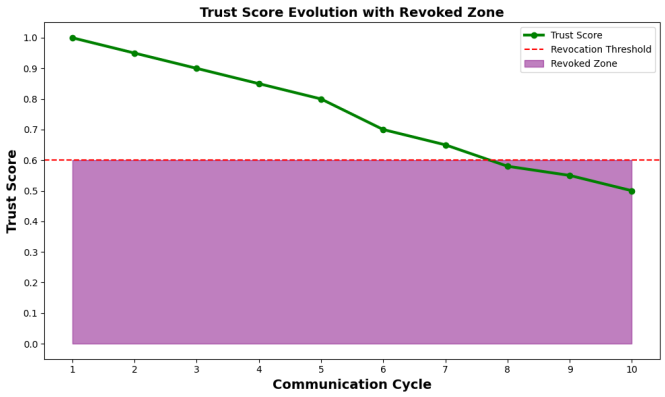

Fig. 3. Visual plot of system trust score evolution over communication cycles. The revoked zone is clearly shaded in purple below the red dashed revocation threshold line at 0.6.

Fig 3 depicts the real-time evolution of the proposed system trust score over 10 behavior cycles, incorporating simulated anomalies. The trust score $\tau_i(t)$ begins at 1.0 and evolves based on behavioral input using:

$$\tau_i(t) = \tau_i(t-1) + \Delta_{\text{normal}} - \Delta_{\text{anomaly}} \tag{10}$$

where $\Delta_{\text{normal}} = 0.02$ is the increment for normal behavior and $\Delta_{\text{anomaly}} = 0.1$ is the penalty for anomalies. The red dashed line in the figure indicates the revocation threshold $\mu_T = 0.6$. A device is flagged for revocation when the trust score falls

below μ_T or the anomaly streak $S_i(t)$ exceeds a set threshold $\mu_2 = 3$:

$$\text{Revoke}(ID_i) \iff \tau_i(t) < \mu_T \quad \text{or} \quad S_i(t) > \mu_2 \tag{11}$$

The anomaly streak counter is updated as follows:

$$S_i(t) = \begin{cases} S_i(t-1) + 1, & \text{if anomaly at time } t \\ 0, & \text{if normal behavior} \end{cases} \tag{12}$$

To visually reinforce the revocation enforcement logic, the revoked zone in the graph is shaded purple to indicate periods when the trust score τ_i breaches the revocation threshold.

Terminal Output

```
[] Keypair generated.
[] Encryption complete.
[] Decryption complete.
[] Shared secrets match
[] Normal behavior during cycle 1
[] Normal behavior during cycle 2
[] Normal behavior during cycle 3
[] Normal behavior during cycle 4
[] Normal behavior during cycle 5
[] Normal behavior during cycle 6
[] Normal behavior during cycle 7
[] Normal behavior during cycle 8
[] Normal behavior during cycle 9
[] Anomaly detected during cycle 10
[] Final Trust Score: 95
---Serialized Device Identity---
Public Key (hex): 9919192D4DE26417A3645F
844AD8690EC9C00F52A...
Trust Score: 95
{"public_key":"99197323E00D19733ED217B24..",
"trust_score":95}
[] Stored identity to storage.json
--- Trust Score Visualization ---
[] 95%
[] HIGH TRUST
```

B. Compressed Key Encapsulation Delivery Protocol

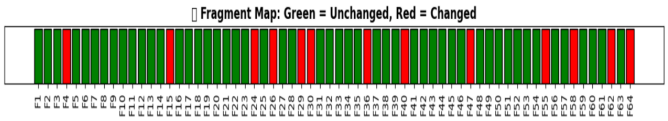

Fig. 4. Fragment Map Diagram showing Changed vs Unchanged Fragments. Fragment Map: Green = Unchanged, Red = Changed

Fig 4, presents the fragmentation visualization where the Kyber512 ciphertext is split into 64 fragments. Green indicates unchanged fragments, while red indicates changed ones across transmissions. This observation reveals that most fragments remain stable, enabling the reuse-aware decoding strategy. By avoiding retransmission of unchanged parts, bandwidth is saved and protocol efficiency is improved. This validates the principle behind selective delta encoding, which forms the basis of the proposed compression strategy.

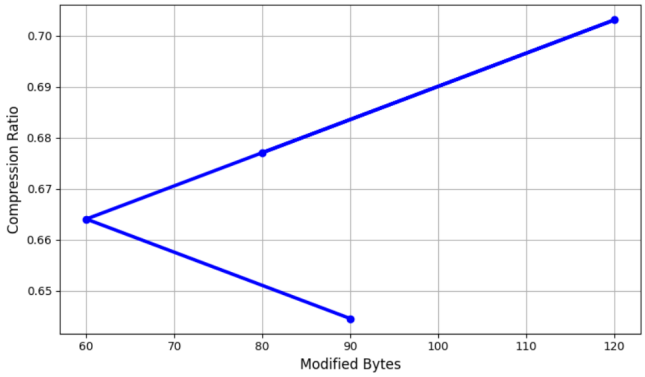

Fig. 5. The Line plot showing the effect of the number of modified bytes on the resulting compression ratio

Fig 5, demonstrates how the number of modified bytes affects the compression ratio. As the mutation rate increases, the compression ratio fluctuates slightly, revealing the system's resilience to minor data changes. The compression ratio R is defined as:

$$R = \frac{\text{Compressed Size}}{\text{Original Size}} \tag{13}$$

Despite slight increases in modified bytes (from 60 to 120), compression remained efficient below 70% of original size, indicating robustness of the reuse-aware scheme under moderate ciphertext changes.

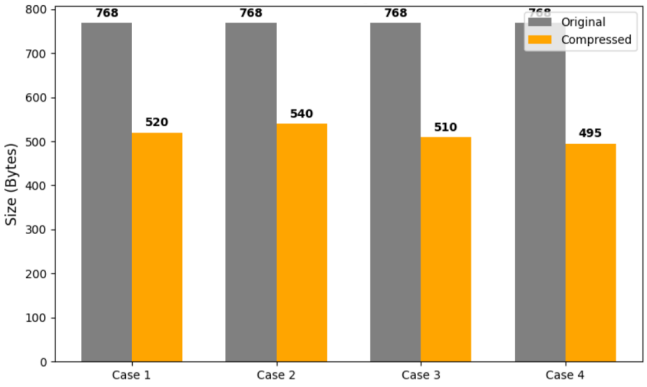

Fig. 6. Original vs Compressed Bar Chart comparing the original ciphertext size with the compressed sizes in four different simulation cases

In Fig 6, a direct comparison of original ciphertext size, 768 bytes and its compressed variants is provided across four simulation cases. The compressed sizes range from 495 to 540 bytes, showing a consistent reduction. The amount of savings Δ is defined as:

$$\Delta = \text{Original Size} - \text{Compressed Size} \tag{14}$$

$$\text{Percentage Savings} = \left(\frac{\Delta}{\text{Original Size}}\right) \times 100 \tag{15}$$

The protocol achieves over 30% reduction in size, which aligns to reduce delivery footprint using fragmentation, delta encoding, and compression.

C. Performance Evaluation

1) Baseline Comparison with Entropy-less Models: To highlight the significance of entropy-seeded identity, Table III depicts the baseline comparison with entropy-less models. We compare with an identity scheme using only device MAC addresses and timestamps.

TABLE III
IDENTITY MODEL COMPARISON

Model	S.R	E.B	Adaptability
MAC + Timestamp (Baseline)	Low	∼32	None
PUF + Metadata (Literature)	Medium	∼64	Static
Ours (Entropy-seeded)	**High**	**128+**	**Real-time**

*SR-Spoof Resistance; *EB- Entropy Bits

Our entropy rooted model offers superior spoof resistance and enables trust scoring over time as key advantage over static identity approaches.

2) Compression Performance and Key Delivery Overhead: We evaluate the impact of delta-based ciphertext compression on post-quantum key encapsulation using CRYSTALS-Kyber512. Table IV compares the raw Kyber ciphertext size with our proposed compressed delivery scheme.

TABLE IV
CIPHERTEXT SIZE REDUCTION VIA DELTA COMPRESSION (KYBER512)

Scheme	R.S (bytes)	C.S(bytes)	C.R(%)
Kyber512 (baseline)	800	–	–
Kyber512 + ZLIB	800	510	36.3%
Delta-aware Kyber512 (ours)	800	410	**48.75%**

*R.S-Raw Size in bytes; *C.S- Compression Size; *C.R-Compression ratio

Our scheme outperforms generic compression by reusing known ciphertext segments, enabling efficient transmission in IIoT contexts.

3) Latency and CPU Overhead: Table V summarizes the average latency and CPU utilization for key operations under three configurations:

TABLE V
LATENCY AND CPU USAGE COMPARISON

Scheme	KEL(ms)	CPU Usage (%)
Kyber512 (uncompressed)	18.2	24.1
Compressed Kyber512 (ZLIB)	15.4	26.3
Proposed (Delta-aware + Fragmented)	**12.6**	**20.9**

*KEL-Key Exchange Latency (ms)

The proposed system reduces overall key exchange latency by 30.7% over raw Kyber, and 18.2% over ZLIB-only schemes. CPU impact remains within acceptable bounds for IIoT-grade devices.

IV. CONCLUSION

This work addresses the pressing need for scalable and quantum-resilient security in resource-constrained IIoT deployments. We presented and implemented two core components: (1) an entropy-seeded identity generation model that synthesizes biometric, device-level, and behavioral entropy sources to form context-aware, tamper-resistant identities; and (2) a lightweight, delivery-optimized PQC protocol that compresses Kyber512 ciphertexts via delta encoding, fragmentation, and selective reuse. Experimental evaluation on a Raspberry Pi endpoint shows promising performance improvements achieving over 48% reduction in ciphertext size and 30% latency reduction while maintaining cryptographic integrity. To complement the identity and delivery stack, a hybrid blockchain-based revocation model was introduced conceptually, offering a vision for full lifecycle trust enforcement. While not yet implemented, its inclusion in the architectural design illustrates the long term scalability of the system and auditability potential. Future work will involve deploying and evaluating the full blockchain-based revocation pipeline across hybrid ledgers and exploring integration with real-time anomaly detection engines for trust scoring.

ACKNOWLEDGMENT

This work was partly supported by the Institute of Information Communications Technology Planning Evaluation(IITP)-Innovative Human Resource Development for Local Intellectualization program grant funded by the Korea government(MSIT)(IITP-2025-RS-2020-II201612, 34%) and ITRC(Information Technology Research Center) grant funded by the Korea government(MSIT)(IITP-2025-RS-2024-00438430, 33%) and by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2018R1A6A1A03024003, 33%)

REFERENCES

[1] I. Analytics, "State of iot—spring 2024 update," *IoT Analytics Research*, 2024, available at: https://iot-analytics.com.

[2] Y. Guo, L. Li, X. Jin, C. An, C. Wang, and H. Huang, "Physical-unclonable-function-based lightweight anonymous authentication protocol for smart grid," *Electronics*, vol. 14, no. 3, p. 623, 2025.

[3] K. Mahmood, S. Shamshad, M. A. Saleem, R. Kharel, A. K. Das, S. Shetty, and J. J. Rodrigues, "Blockchain and puf-based secure key establishment protocol for cross-domain digital twins in industrial internet of things architecture," *Journal of Advanced Research*, vol. 62, pp. 155–163, 2024.

[4] J. Fan, S. Tu, H. Wang, and Z. Liu, "A lightweight puf-based authentication protocol for m2m communications in industrial iot," in *Proceedings of the 2024 14th International Conference on Communication and Network Security*, 2024, pp. 189–193.

[5] M. G. de la Torre, I. M. Sandoval, G. F. de Abreu, and L. H. Encinas, "Post-quantum wireless-based key encapsulation mechanism via crystals-kyber for resource-constrained devices," *IEEE Access*, 2025.

[6] J. S. Sánchez, "Analysis and evaluation of the impact of post-quantum cryptography at the edge of iot," Ph.D. dissertation, Universidad Politécnica de Madrid Madrid, 2024.

[7] Y. Long, C. Peng, W. Tan, and Y. Chen, "Blockchain-based anonymous authentication and key management for internet of things with chebyshev chaotic maps," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 5, pp. 7883–7893, 2024.

[8] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50–57, 2018.

[9] B. Yuan, F. Wu, and Z. Zheng, "Post quantum blockchain architecture for internet of things over ntru lattice," *PLOS ONE*, vol. 18, no. 2, pp. 1–21, 02 2023.